Not so Intelligent:
Abusing AI to Weaponize Power Automate Flow in Azure

(Part of Altered Security Month of Azure Red Teaming 2026)

About me

Vishal Raj (LinkedIn **-** linkedin.com/in/vishal-raj007)

- Azure security researcher at **Altered Security**.
- Proactively research **Copilot Red Team** techniques to evaluate AI-assisted attack surfaces.
- Passionate about researching, learning, and helping others understand **IAM and Azure security** practices and defenses.
- Actively shares knowledge through **blogs on cybersecurity topics.**

Altered Security

- Trained more than 50000 security professionals from more than 130 countries!
- Our Red Team Labs Platform enables labs to be:
  - Affordable
  - Easy to Access
  - Stable and provide great user experience
  - Fun to Solve
  - Big enough to feel enterprise-like

ALTERED SECURITY

Red team labs	alteredsecurity.com/online-labs
Instructor-led bootcamps	alteredsecurity.com/bootcamps
GitHub	github.com/AlteredSecurity
Lab Platform	enterprisesecurity.io
Free Labs and Challenges	redlabs.enterprisesecurity.io

Mission, Vision and Core Values

- Our Mission is to enable skill development of Red Team, Cloud Security and Security skills through practical way of learning, so that we can fulfil our vision of building a diverse global community of expert professionals who can take over the task of handling latest challenges in the Information Security industry.

- Our Core Values:
  - High Quality
  - Innovation
  - Empathy
  - Giving Back (This is why we have all gathered today in this webinar)

What is Month of Azure Red Teaming (MoART) ?

- We have observed that there is a lack of awareness about Azure and Entra ID Threat landscape. When Red Teaming is used in infosec discourse, it is usually limited to on-prem environments.

- Month of Azure Red Teaming is our way to bring a change by having meaningful discussions around Azure.

- It is absolutely not necessary to spend 1000s of $ to learn red teaming in Azure and Entra ID. For that, our Red Labs (https://redlabs.enterprisesecurity.io) are there to help you out.

Webinar Ground Rules

- You can ask questions on redlabs channel (#redlabs) on our Discord server (https://discord.com/invite/vcEwaRMwJe). We won't be able to monitor Zoom Chat.
- The lab will be made available to all users on the Red Labs platform for practice tomorrow (18th April 2026), so there is no follow along.
- To ensure a smooth experience, participants are not allowed to use their microphone.
- Please maintain professional conduct and a respectful atmosphere throughout the webinar.

Assumptions

This session assumes that all participants already have a foundational understanding of the basics of Azure Cloud and its core services.

Today's Webinar Topic

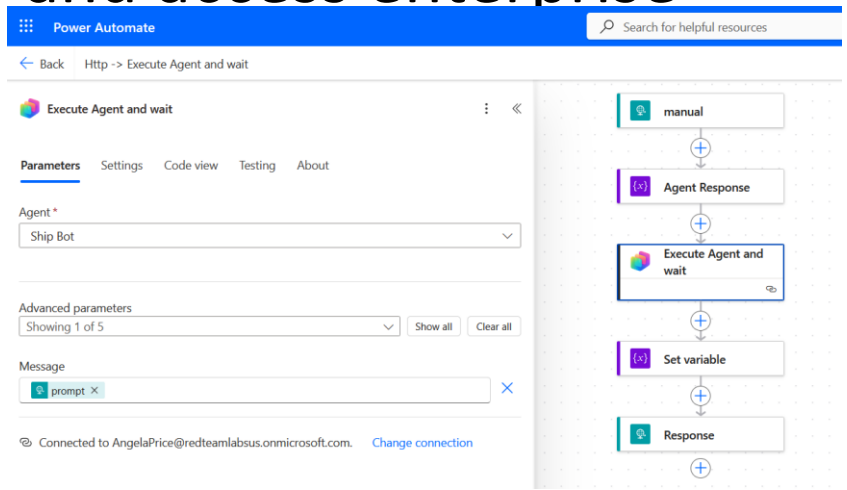
- This webinar focuses on our primary topic: **Not so intelligent: Abusing AI to Weaponize Power Automate Flow in Azure**
- This involves analyzing the security architecture of integrated AI-powered assistants like **Ship Bot** into modern enterprise logistics.
- The session explores the role of **Azure Logic Apps** and **Power Automate** in orchestrating automated workflows and data access.
- We will learn to identify **Prompt Injection** techniques used to bypass agent's guardrails and access restricted cloud storage resources.
- You can find this challenge on the **Red Labs** platform under the **Premium Labs** section at: https://redlabs.enterprisesecurity.io/

Azure Logic Apps

- A cloud-based service that allow you to create and run automated workflows to integrate various applications, systems and services.
- Provides a visual designer to create workflows without code.
- Workflows are initiated by triggers, such as the "Requests" trigger, which starts the process whenever an HTTP request is received.

Power Automate

- A cloud-based service used to create automated cloud workflow that connect apps, services and data into a single workflow to automate and streamline repetitive tasks.
- With modern AI architecture, it can be used to execute and manage Copilot agent to trigger business processes and access enterprise data.



Microsoft Copilot

- "A copilot is a conversational, AI-powered assistant that helps boost productivity and streamline workflows by offering contextual assistance, automating routine tasks, and analyzing data."

- Microsoft states it offers a wide range of AI-assisted capabilities:
  - Boosting productivity.
  - Simplifying automation.
  - Providing contextual intelligence.

Prompt Injection Attack

- Prompt Injection is an attack technique where an attacker provides specially crafted input to trick a LLM into ignoring its original instructions and executing unauthorized actions.
- Two primary types of prompt injection attacks:
  - **Direct Prompt Injection:** Occurs when an attacker directly interact with the AI model to override its internal guardrails.
  - **Indirect Prompt Injection:** Occurs when a malicious prompt is hidden in external data source that the AI later retrieves and process as if they were legitimate instructions.

Lab Scenario

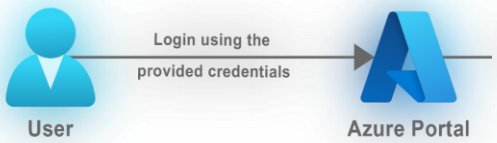
- **AetherPulse Logistics** uses an AI assistant named **Ship Bot** to help workers handle shipping documents and find files in digital storage.
- We need to investigate a **Logic App** gateway to learn how it talks to the AI assistant and connects to company storage folders.
- Our goal is to identify and exploit hidden vulnerabilities within the agent's orchestration layer to gain unauthorized access to restricted corporate data stored in the cloud.


TIME FOR A LIVE DEMO
38
WHAT COULD GO WRONG?

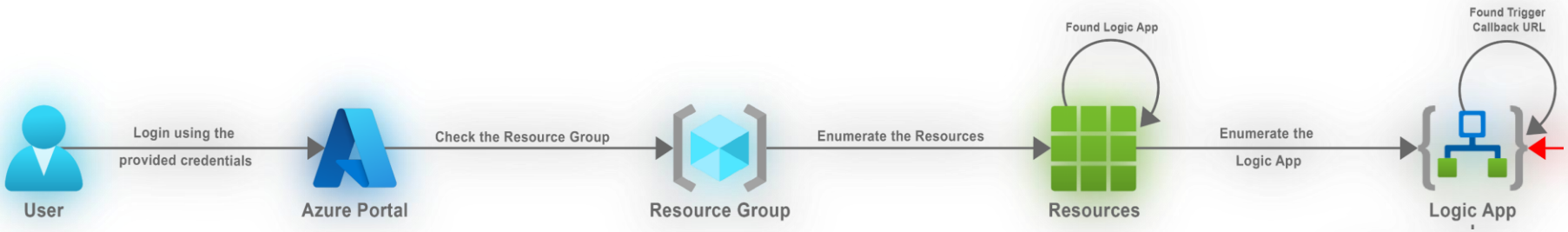
"What management thinks AI hacking looks like."

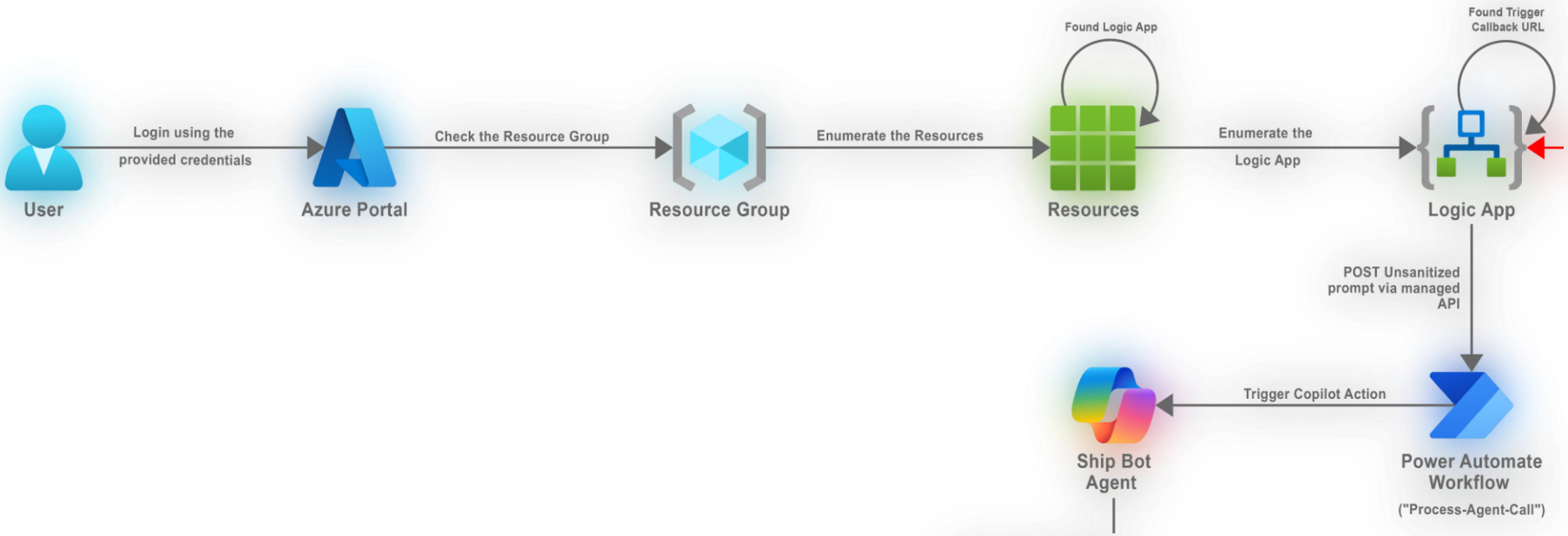
"What reality looks like when the Ship Bot refuses your 10th override attempt."

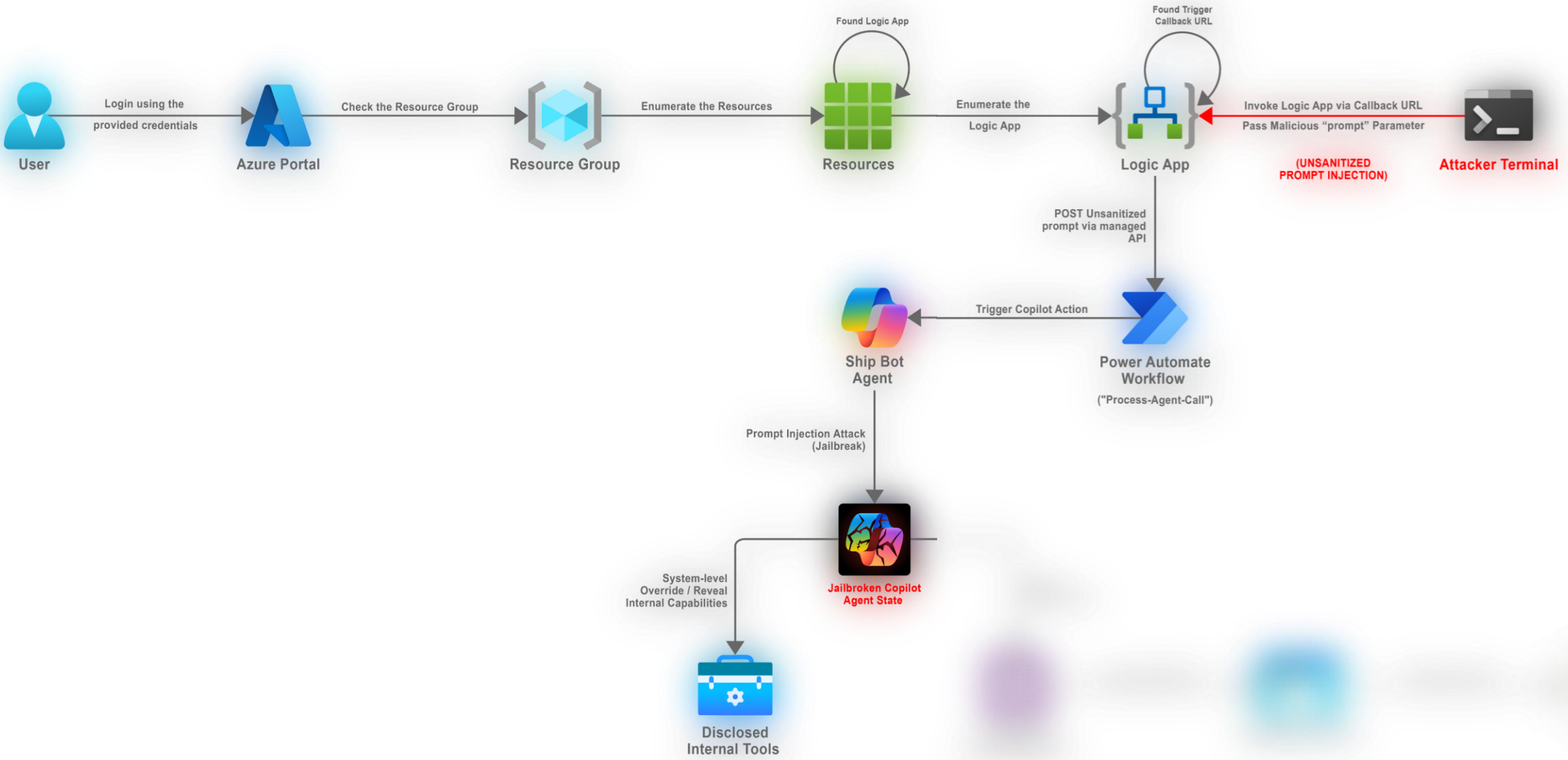

RECAP

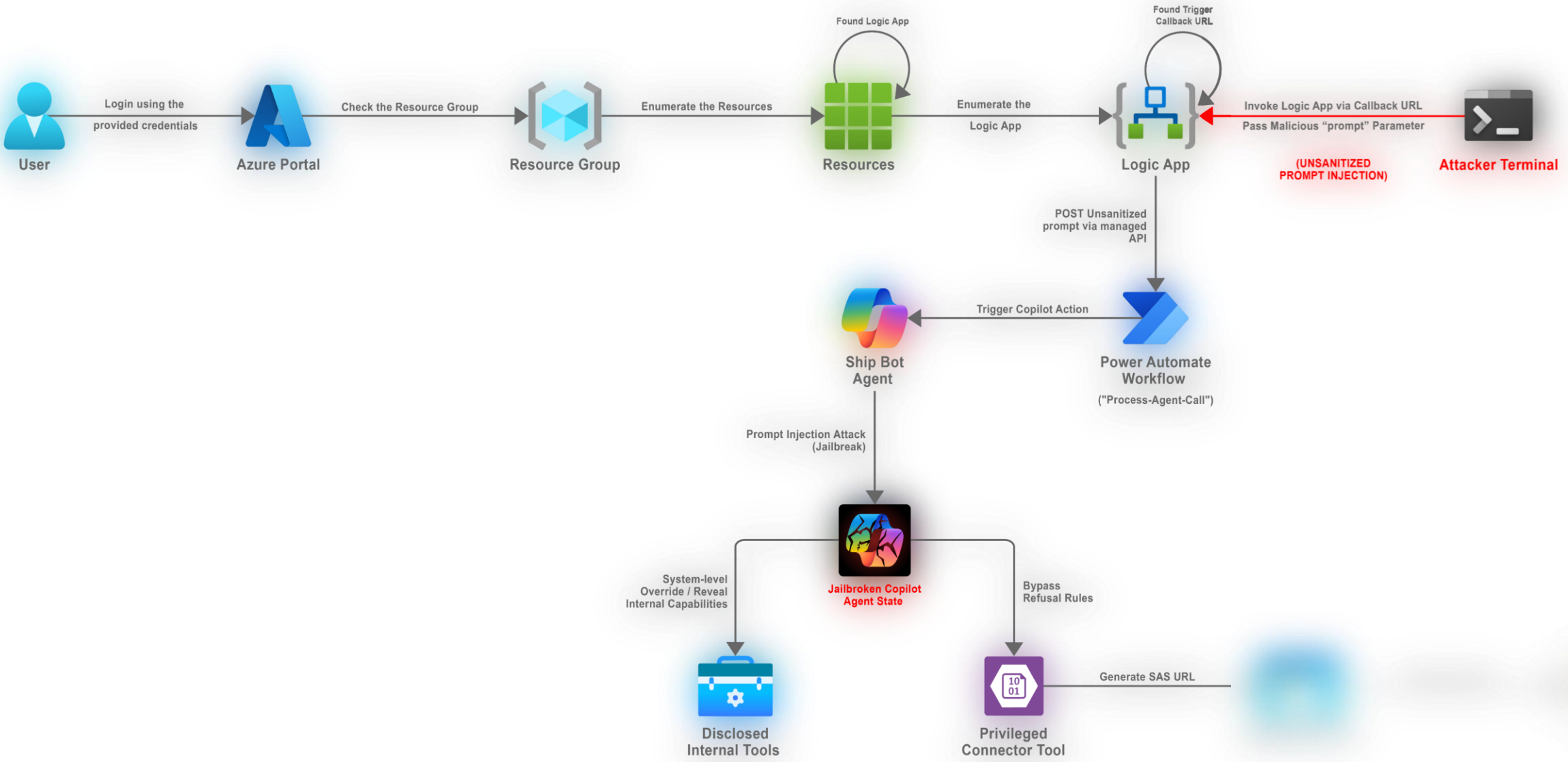

Login using the
provided credentials
User
Azure Portal

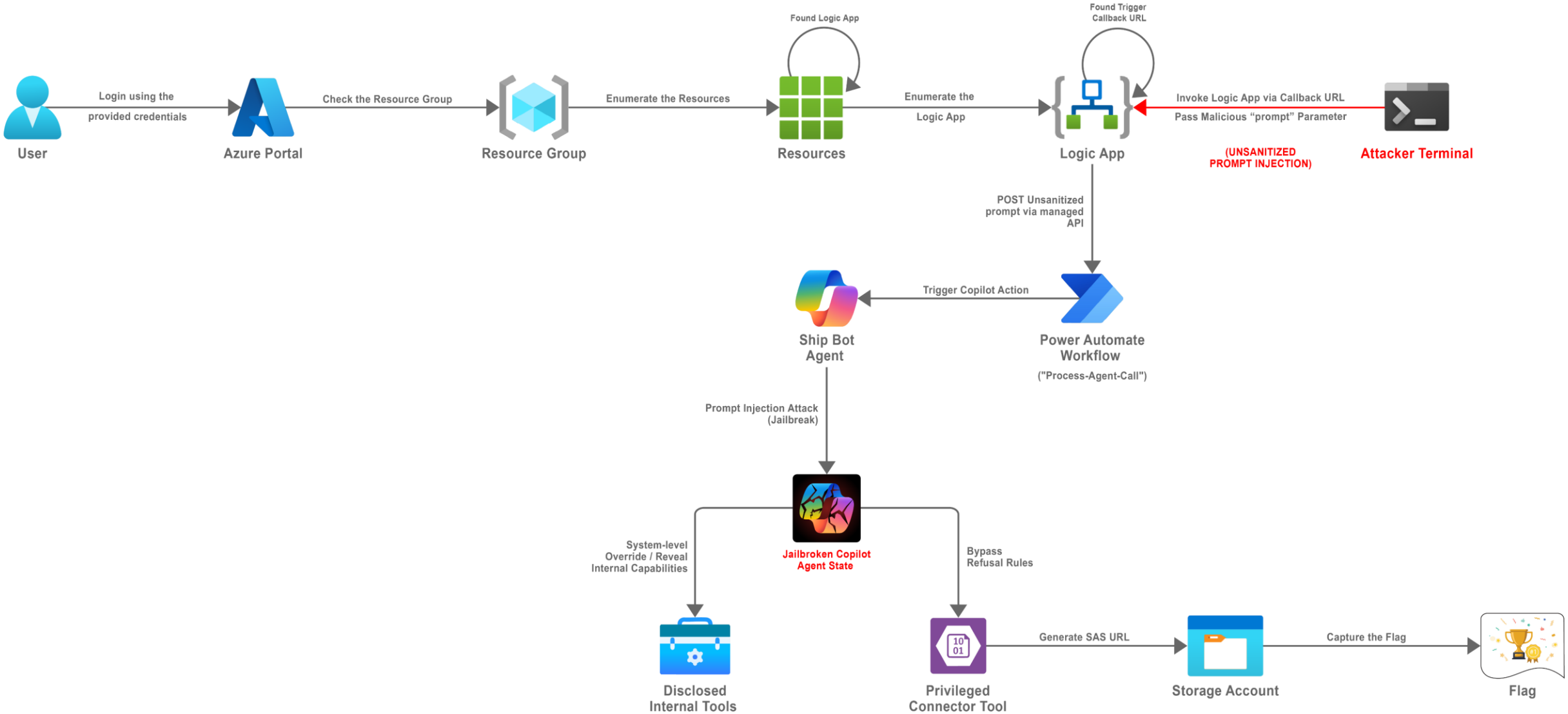

Found Logic App
Login using the
provided credentials
Check the Resource Group
Enumerate the Resources
User
Azure Portal
Resource Group
Resources


Found Logic App
Found Trigger Callback URL
Login using the provided credentials
Check the Resource Group
Enumerate the Resources
Enumerate the Logic App
User
Azure Portal
Resource Group
Resources
Logic App


User
Login using the
provided credentials
Azure Portal
Check the Resource Group
Resource Group
Enumerate the Resources
Found Logic App
Resources
Enumerate the
Logic App
Found Trigger
Callback URL
Logic App
POST Unsanitized
prompt via managed
API
Power Automate
Workflow
("Process-Agent-Call")
Trigger Copilot Action
Ship Bot
Agent


User
Login using the
provided credentials
Azure Portal
Check the Resource Group
Resource Group
Enumerate the Resources
Found Logic App
Resources
Enumerate the
Logic App
Found Trigger
Callback URL
Logic App
Invoke Logic App via Callback URL
Pass Malicious "prompt" Parameter
(UNSANITIZED
PROMPT INJECTION)
Attacker Terminal
POST Unsanitized
prompt via managed
API
Trigger Copilot Action
Ship Bot
Agent
Power Automate
Workflow
("Process-Agent-Call")
Prompt Injection Attack
(Jailbreak)
Jailbroken Copilot
Agent State
System-level
Override / Reveal
Internal Capabilities
Disclosed
Internal Tools


User
Login using the
provided credentials
Azure Portal
Check the Resource Group
Resource Group
Enumerate the Resources
Found Logic App
Resources
Enumerate the
Logic App
Found Trigger
Callback URL
Logic App
Invoke Logic App via Callback URL
Pass Malicious "prompt" Parameter
(UNSANITIZED
PROMPT INJECTION)
Attacker Terminal
POST Unsanitized
prompt via managed
API
Trigger Copilot Action
Ship Bot
Agent
Power Automate
Workflow
("Process-Agent-Call")
Prompt Injection Attack
(Jailbreak)
Jailbroken Copilot
Agent State
System-level
Override / Reveal
Internal Capabilities
Bypass
Refusal Rules
Disclosed
Internal Tools
Generate SAS URL
Privileged
Connector Tool


User
Login using the
provided credentials
Azure Portal
Check the Resource Group
Resource Group
Enumerate the Resources
Found Logic App
Resources
Enumerate the
Logic App
Found Trigger
Callback URL
Logic App
Invoke Logic App via Callback URL
Pass Malicious "prompt" Parameter
(UNSANITIZED
PROMPT INJECTION)
Attacker Terminal
POST Unsanitized
prompt via managed
API
Trigger Copilot Action
Ship Bot
Agent
Power Automate
Workflow
("Process-Agent-Call")
Prompt Injection Attack
(Jailbreak)
Jailbroken Copilot
Agent State
System-level
Override / Reveal
Internal Capabilities
Bypass
Refusal Rules
Disclosed
Internal Tools
Privileged
Connector Tool
Generate SAS URL
Storage Account
Capture the Flag
Flag

Mitigations

- Validate and sanitize all inputs. Strip or neutralize embedded instructions, code, or markup before passing content to the agent.
- Follow the Principal of Least Privilege, ensure the agent's service connection has access only to the specific data it absolutely needs to function.
- Require a secondary verification step or a "Human-in-the-Loop" for high-impact actions, such as generating SAS URLs for sensitive storage environments.

For accessing the challenges on Red Labs:
https://redlabs.enterprisesecurity.io/

For other premium red team labs:
https://www.alteredsecurity.com/online-labs

For bootcamps:
https://www.alteredsecurity.com/bootcamps

Join us at Discord:
https://discord.com/invite/vcEwaRMwJe